**AMRUTHESH**

**241059041**

**CRYPTOLOGY**

**M.E – CYBER SECURITY**

**Threat Modelling for a Hypothetical Online Banking System**.

**1. Assets**

These are valuable resources within the online banking system that need protection:

* **Customer data** (e.g., personal identification information, account numbers, transaction histories)
* **Bank accounts** (e.g., customer savings, checking accounts)
* **Financial transactions** (e.g., fund transfers, bill payments)
* **Authentication credentials** (e.g., passwords, OTPs, biometric data)
* **Bank servers and infrastructure**
* **Third-party payment integrations**

**2. Threats**

These are potential circumstances or events that could exploit a vulnerability:

* **Unauthorized access to accounts** (e.g., due to weak or stolen passwords)
* **Data breaches** (e.g., exposure of customer data due to an insecure database)
* **Phishing attacks** (e.g., attackers tricking users into revealing login credentials)
* **Man-in-the-middle (MITM) attacks** (e.g., interception of communications between the user and the bank)
* **Denial-of-service (DoS) attacks** (e.g., attackers flooding the system, preventing legitimate users from accessing services)
* **Insider threats** (e.g., bank employees misusing their access)
* **Ransomware attacks** (e.g., attackers encrypting customer data and demanding ransom)

**3. Vulnerabilities**

These are weaknesses in the system that could be exploited:

* **Weak encryption protocols** used for protecting communication or stored data
* **Unpatched software** on bank servers or client systems
* **Inadequate access control policies** allowing excessive permissions
* **Weak or absent multifactor authentication (MFA)**
* **Phishing susceptibility** among customers
* **Outdated or vulnerable third-party APIs**

**4. Attacks**

These are specific tactics that adversaries might use to exploit vulnerabilities:

* **SQL Injection**: Attackers injecting malicious queries to retrieve or alter database information.
* **Credential stuffing**: Using previously breached credentials to gain access to bank accounts.
* **Cross-site scripting (XSS)**: Exploiting web vulnerabilities to execute scripts in a user's browser.
* **Social engineering**: Manipulating customers or employees to gain access to sensitive systems.
* **Brute force attacks**: Repeatedly trying passwords or PINs until successful.
* **Distributed Denial-of-Service (DDoS)**: Flooding the server with massive traffic to disrupt services.

**5. Risks**

These are potential consequences if the threats materialize:

* **Financial loss** for both the bank and its customers
* **Reputation damage** leading to loss of customer trust
* **Legal and regulatory penalties** due to non-compliance with data protection laws (e.g., GDPR)
* **Service outages** causing disruption to customer banking
* **Loss of sensitive data** leading to identity theft
* **Customer attrition** due to loss of trust

**6. Exploits**

These are methods by which vulnerabilities might be abused:

* **Malware or phishing kits** used to steal credentials or distribute ransomware
* **Automated bots** carrying out brute force or credential stuffing attacks
* **MITM tools** for intercepting unencrypted communication
* **Exploiting API vulnerabilities** to retrieve unauthorized data

**7. Impact**

The effects of successful attacks can be devastating:

* **Loss of customer funds** through fraudulent transactions
* **Compromise of personal and financial data** leading to identity theft
* **Operational disruption** leading to loss of services for all users
* **Regulatory fines and lawsuits** due to data breaches or failure to protect assets
* **Long-term damage to the brand** and erosion of customer confidence
* **High remediation costs** for incident response, compensation, and system upgrades

**8. Solution:**

By identifying these threats and their potential impacts, the bank can take preventive measures such as implementing stronger authentication protocols (e.g., multifactor authentication), regularly patching systems, educating users, and employing monitoring tools to detect and mitigate malicious activity.